ЦИФРОВА ОСВІТЯНСЬКА СПРОМОЖНІСТЬ ЩОДО ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ТА КОНФІДЕНЦІЙНИХ ДАНИХ

Павловська Тетяна Тарасівна

магістрантка спеціальності 014.09 «Середня освіта (Інформатика)»,

Тернопільський національний педагогічний університет імені Володимира Гнатюка,

kavkatania@gmail.com

Балик Надія Романівна

Кандидат педагогічних наук, доцент кафедри інформатики та методики її навчання

Тернопільський національний педагогічний університет імені Володимира Гнатюка

nadbal@fizmat.tnpu.edu.ua

Наші дослідження показують, що цифровий досвід учнів та студентів сильно залежить від впевненості та можливостей їх викладачів і удосконалення їх педагогічної майстерності впродовж професійної діяльності [2–4]. Це робить цілеспрямований та гнучкий постійний професійний розвиток учительського персоналу ключовим пріоритетом, у галузі захисту конфіденційної інформації, зокрема [5]. Нова редакція Закону України «Про інформацію», як базового нормативно-правового акту в інформаційній сфері, надає нове визначення інформації – як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [1].

Однак деяка інформація є особливо чутливою — наприклад, інформація, яка загалом не відома в галузі, наша інтелектуальна власність або навіть комерційна таємниця.

Різні помилкові ситуації трапляються: ноутбуки викрадають, мобільні пристрої втрачають, електронні листи надсилають не тим одержувачам, але якщо учень, студент, викладач дотримується правильних процедур, то такі «аварії» не повинні ставатись.

Розглянемо, що потрібно зробити для захисту своєї конфіденційної інформації та конфіденційних даних:

- Визначити класифікацію даних, які обробляються.

- Використати протоколи обробки для цього класу даних, щоб:
    - ділитися даними належним чином;
    - безпечно зберігати дані;
    - правильно розпоряджатися даними.

Також необхідно зауважити, що за деяких обставин розголошення конфіденційної інформації вимагається законодавством.

Присвоєння рівня класифікації інформації — це перший крок до належного захисту особистої інформації. Класифікація — це ділове рішення, засноване на тому, наскільки чутливою є інформація. Після того, як інформація була класифікована, її потрібно правильно позначити, щоб кожен, хто працює з нею, усвідомлював рівень її чутливості. Кожен повинен знати класифікацію інформації, яку він обробляє, та належним чином поводитися з нею.

Існує чотири основних класи інформації:

Публічна — інформація, якою можна вільно ділитися з будь-якою особою чи групою.

Внутрішня — потенційно конфіденційна інформація, яка не повинна передаватися за межами організації.

Конфіденційна — інформація (в усній, письмовій або електронній формі), яка може негативно вплинути на працівників, приватних осіб або на бізнес, якщо буде розкрита несанкціонованим сторонам. Наприклад, бізнес-стратегії, маркетингові плани, технології виробництва тощо.

Обмежена — інформація, яку ми зобов'язані підтримувати та захищати відповідно до законодавства чи закону. Комерційну таємницю також іноді класифікують як інформацію обмеженого доступу.

Інформаційна політика регулює зовнішні комунікації в усіх формах засобів масової інформації, включаючи друковані, онлайн-платформи та публічні форуми. Використовуючи систему електронних комунікацій, включаючи інтернет, або займаючись діяльністю у соціальних мережах, людина не повинна надсилати або іншим чином розголошувати конфіденційну інформацію, комерційну таємницю чи інші конфіденційні дані. Ніколи не можна обговорювати конфіденційну або обмежену інформацію в громадських місцях

або в соціальних розмовах, і завжди використовувати в обговореннях «кодові назви».

Перед тим, як надіслати електронне повідомлення, слід ще раз перевірити одержувача, перш ніж натискати кнопку надсилання — не тільки може бути неприємно, якщо повідомлення надіслано не тій людині, але це також може призвести до ненавмисного розголошення конфіденційної інформації. Якщо потрібно надіслати вкладення, яке містить конфіденційну або обмежену інформацію, необхідно переконатися, що файл захищений паролем.

Розглядати можливість вставити адресу електронної пошти одержувача слід лише після того, як буде готовність надіслати електронне повідомлення. Ніколи не слід вважати, що внутрішні чи зовнішні повідомлення є приватними та конфіденційними, навіть якщо вони позначені як такі. Інтернет не є захищеним засобом спілкування, і треті сторони можуть мати доступ змінювати повідомлення, які були надіслані або отримані. Не слід надсилати в електронному листі будь-якої інформації, яку б кореспондент не хотів, щоб вона була загальнодоступною. Питання делікатного або особистого характеру не повинні передаватися електронною поштою.

Особливо обережним треба бути, використовуючи соціальні медіа — навіть коли відбувається спілкування у чаті зі своїми колегами; завжди слід пам’ятати про потенційні особисті та корпоративні ризики. Коли людина публікує повідомлення за допомогою соціальних мереж, вона повинна припустити, що робить публічну заяву, навіть якщо встановлено налаштування конфіденційності лише для відомих осіб. Такі повідомлення не будуть приватними та можуть передаватися третім особам без особистої згоди. Після розміщення конфіденційної інформації (або образливої, або наклепницької інформації) її неможливо стерти, і це може спричинити шкоду або відповідальність як для фірми, так і для людини особисто. Ніколи не слід обговорювати внутрішню, конфіденційну або обмежену інформацію в соціальних мережах.

Конфіденційність внутрішніх комунікацій може бути забезпечена лише в тому випадку, якщо вони надсилаються внутрішньою поштою компанії у

належним чином позначеному та запечатаному конверті, доставляються особисто з рук в руки або включаються в захищений паролем інтернет-документ. За жодних обставин інформація конфіденційного характеру не повинна розміщуватися в інтернеті. Слід проявляти ту саму обережність, користуючись телефоном або факсом, як при використанні електронної пошти чи інших форм письмового спілкування.

Вибір рівня класифікації, який застосовуватиметься до приватних даних, є діловим рішенням, заснованим на тому, наскільки важливі ці дані. Чим чутливіша інформація, тим вищий рівень класифікації та необхідний більший захист. Класифікуючи інформацію, а потім дотримуючись встановлених правил, кожен учень, студент, викладач може захистити себе та свій навчальний заклад у випадку аварії безпеки. Сьогоднішні технології дають можливість кожному забезпечити правильний рівень захисту конфіденційних даних.

Список використаних джерел

1. Нове в законодавстві про інформацію – https://minjust.gov.ua/m/str_35738

2. Балик Н. Р., Шмигер Г. П. Аспекти впровадження моделі навчання протягом життя у smart-університеті. Молодий вчений. 2017. №4. С. 347–350

3. Балик Н.Р., Шмигер Г.П. Технологія змішаного навчання у процесі вивчення сучасних інформаційних технологій студентами хіміко-біологічних факультетів педагогічних університетів. Наукові записки ТНПУ ім. Володимира Гнатюка. Серія: Педагогіка. Тернопіль, 2011. №1. С.9–17.

3. Балик Н.Р., Шмигер Г.П. Формування інформаційно-освітнього простору курсу «Сучасні інформаційні технології в навчальному процесі» для студентів непрофільних спеціальностей з використанням технологій Веб 2.0. Наукові записки ТНПУ ім. Володимира Гнатюка. Серія: Педагогіка. Тернопіль, 2010. №1. С.140–147.

5. Олексюк В.П., Олексюк О.Р. Стан сформованості компетентностей з інформаційної безпеки майбутніх учителів інформатики. Інформаційні технології і засоби навчання. 2017. № 62(6). С. 277–291.